ALEC American Legislative Exchange Council

LIMITED GOVERNMENT • FREE MARKETS • FEDERALISM

2013 STATES AND NATION POLICY SUMMIT
CONSUMER PROTECTION, CRITICAL INFRASTRUCTURE, AND SECURITY TECHNOLOGIES SUBCOMMITTEE
MEETING TENTATIVE AGENDA
Wednesday, December 4th

9:30am-10:10am – Subcommittee Meeting – Room: Wilson/Roosevelt

- **Welcome and Introductions**

- **Policy Discussion**
  - Statement of Principles for Cybersecurity – *Sen. Joel Anderson (CA) and Rep. Blair Thoreson (ND)*
  - Statement of Principles for the Electronic Communications Privacy Act – *Rep. Garry Smith (SC)*

- **Presentation** — *"Critical Infrastructure: securing the nation's backbone"*
  - Kirstjen Nielsen of Sunesis Consulting Inc.

- **Adjourn**

DRAFT

ALEC American Legislative Exchange Council

LIMITED GOVERNMENT • FREE MARKETS • FEDERALISM

2013 STATES AND NATION POLICY SUMMIT
CONSUMER PROTECTION, CRITICAL INFRASTRUCTURE AND SECURITY TECHNOLOGIES SUBCOMMITTEE
SPEAKER BIOGRAPHIES
Wednesday, December 4th

SPEAKERS

The Honorable Kirstjen Nielsen – *President, Sunesis Consulting, LLC*

The Honorable Kirstjen Nielsen is an expert in homeland and national security policy, strategy, and assessment, with a focus in the areas of infrastructure protection, cybersecurity, response and incident management, information sharing, risk assessment and risk management, trend analysis, organizational development, stakeholder requirement analysis, outreach and communications, and training and exercise programs. As President of Sunesis Consulting, LLC, Ms. Nielsen currently advises senior Federal, State, local, and foreign government officials on the development and execution of strategies, policies, plans, tools and tabletop exercises to prepare for all hazards. Ms. Nielsen also advises senior private sector officials on a variety of homeland security issues, assesses various entities' preparedness for adverse events and develops recommendations to address any gaps or inefficiencies. Prior to founding Sunesis Consulting, Ms. Nielsen was the General Counsel and President of the Homeland Security and Private Sector Preparedness practice at Civitas Group llc, where, in addition to her work with governments, Ms. Nielsen was instrumental in assessing the legislative and policy landscape for companies looking to enter the homeland security market, expand their presence or develop new homeland security related technologies or capabilities.

Prior to her work at Civitas Group, Ms. Nielsen was commissioned by President George W. Bush to serve as Senior Director and Special Assistant to the President for Prevention, Preparedness, and Response on the White House Homeland Security Council (HSC), where her responsibilities included the development, coordination, and oversight of U.S. Government homeland security policy and the development of numerous Presidential homeland security policy documents on issues ranging from cybersecurity to public alert and warning to improvised explosive devices to the information sharing environment. Prior to her service on the staff of the HSC, Ms. Nielsen created and managed the Offices of Legislative Policy and Government Affairs at the Transportation Security Administration, developing transportation security related policy and drafting legislation relating to security background checks, credentialing, passenger pre-screening, surface transportation and security funding. Ms. Nielsen previously practiced corporate transactional law for Haynes and Boone, LLP and worked for Senator Connie Mack III on defense, aviation, foreign affairs and government affairs issues.

Ms. Nielsen is a Senior Fellow at the Homeland Security Policy Institute at the George Washington University, a Member of the World Economic Forum's Global Agenda Council on Catastrophic Risks, serves on the Homeland Security Advisory Council for Strategic and Global Security Programs at Penn State, and serves on the Center for Naval Analysis Safety and Security Advisory Board. Ms. Nielsen has guest lectured at the National Defense University on a variety of infrastructure protection issues, and at the George Washington University on the

homeland security policy process and Hurricane Katrina lessons learned. Ms. Nielsen has also written articles, served on conference panels (e.g., ISC-West, G-First) and given speeches at homeland security conferences and forums on homeland security preparedness issues and cybersecurity, including giving a presentation on catastrophic risk at the World Economic Forum's (WEF) Advisory Meting on Global Risks, moderating the WEF-Organization of American States' Cyber Security and Its Implications for the Economy and the Financial Sector Conference, and giving a key-note speech at the Penn State Intelligence Community Centers of Academic Excellence Symposium. Ms. Nielsen is a Member of the State of Texas Bar, has Top Secret Clearance and is eligible for SCI Clearance.

ALEC American Legislative Exchange Council

LIMITED GOVERNMENT • FREE MARKETS • FEDERALISM

DRAFT STATEMENT OF PRINCIPLES FOR CYBERSECURITY

WHEREAS, it is the mission of the American Legislative Exchange Council (ALEC) to advance the principles of free markets, limited government and federalism; and

WHEREAS, effective cybersecurity is essential for the proper function of government and continued growth of the economy in cyberspace; and

WHEREAS, cyber challenges could pose an existential threat to the US economy, our national security apparatus and public health and safety;

THEREFORE, LET IT BE RESOLVED, that ALEC supports the following principles in formulating effective government policy regarding cybersecurity:

1. ***Effective cybersecurity measures reflect the global, borderless, and interconnected nature of cyberspace***

Cyberspace is a global and interconnected system of networks and users that spans geographic borders and traverses national jurisdictions. While recognizing government's important role to protect its citizens, the state and the U.S. governments should exercise leadership in encouraging the use of bottom-up, industry-led, and globally-accepted standards, best practices, and assurance programs to promote security and interoperability. We must also collaborate with trusted allies both to share information and to bolster defenses.

2. ***Effective cybersecurity measures are capable of responding and rapidly adapting to new technologies, consumer preferences, business models, and emerging threats***

Cyberspace is full of innovation and dynamism, with rapidly changing and evolving technologies. Cybersecurity measures must be equally dynamic and flexible to effectively leverage new technologies and business models, and changing consumer preferences, and address new, ever-changing threats.

3. ***Effective cybersecurity measures focus directly on threats and bad actors***

In cyberspace, as in the physical world, adversaries use instruments (in this case, technology and communications) to carry out crime, espionage, or warfare. Cybersecurity measures must enable governments to better use current laws, regulations, efforts, and information sharing practices to respond to cyber bad actors, threats, and incidents domestically and internationally.

4. ***Effective cybersecurity measures focus on awareness***

DRAFT

Cyberspace's owners include all who use it: consumers, businesses, governments, and infrastructure owners and operators. Cybersecurity measures must help these stakeholders to be aware of the risks to their assets, property, reputations, operations, and sometimes businesses, and better understand their important role in helping to address these risks. Industry should lead the way in sharing information with the appropriate government entities following an attack and collaborating with others in the private sector to share best practices.

5. ***Effective cybersecurity measures emphasize risk management***

Cybersecurity is not an end state. Rather, it is a means to achieve and ensure continued trust in various technologies and communications networks that comprise the cyber infrastructure. Cybersecurity measures must facilitate an organization's, whether it is the government or a private entity, ability to properly understand, assess, and take steps to manage ongoing risks in this environment.

6. ***Effective cybersecurity measures build upon public-private partnerships, existing initiatives, and resources***

Partnerships between government and industry has provided leadership, resources, innovation, and stewardship in every aspect of cybersecurity since the origin of the Internet. Cybersecurity efforts are most effective when leveraging and building upon these existing initiatives, investments, and partnerships.

DRAFT

ALEC American Legislative Exchange Council

LIMITED GOVERNMENT • FREE MARKETS • FEDERALISM

STATEMENT OF PRINCIPLES FOR ELECTRONIC COMMUNICATIONS PRIVACY ACT REFORM

WHEREAS, it is the mission of the American Legislative Exchange Council (ALEC) to advance the principles of free markets, limited government, and federalism, and;

WHEREAS, it is the mission of ALEC's Task Force for Communications and Technology to advance these principles in order to promote economic growth, freedom of technology, and innovation through public policy, and;

WHEREAS, the federal Electronic Communications Privacy Act (ECPA) is the primary federal law that specifies standards for law enforcement access to electronic communications and associated data, affording important privacy protections to subscribers of emerging wireless and Internet technologies, and;

WHEREAS, the statute has not undergone a significant revision since it was enacted in 1986, and;

WHEREAS, technology has advanced dramatically since 1986, and ECPA has been outpaced, and;

WHEREAS, ECPA is now a patchwork of confusing standards that have been interpreted inconsistently by the courts, creating uncertainty for both service providers and law enforcement agencies, and;

WHEREAS, ECPA can no longer be applied in a clear and consistent way, and, consequently, the vast amount of personal information generated by today's digital communication services may no longer be adequately protected, and;

WHEREAS, ECPA must be flexible enough to allow law enforcement agencies and services providers to work effectively together to combat increasingly sophisticated criminals, and;
WHEREAS, ALEC is a member of Digital Due Process, a diverse coalition of privacy advocates, major companies and think tanks, working together, and;

DRAFT

THEREFORE, LET IT BE RESOLVED, that ALEC supports the Digital Due Process goal of simplifying, clarifying, and unifying the ECPA standards, providing stronger privacy protections for communications and associated data in response to changes in technology and new services and usage patterns, while preserving the legal tools necessary for government agencies to enforce the laws, respond to emergency circumstances and protect the public, and;

LET IT BE FURTHER RESOLVED, that ALEC supports the following guiding principles developed by Digital Due Process in regards to reforming ECPA:

- A governmental entity may require an entity covered by ECPA (a provider of wire or electronic communication service or a provider of remote computing service) to disclose communications that are not readily accessible to the public only with a search warrant issued based on a showing of probable cause, regardless of the age of the communications, the means or status of their storage or the provider's access to or use of the communications in its normal business operations.

- A governmental entity may access, or may require a covered entity to provide, prospectively or retrospectively, location information regarding a mobile communications device only with a warrant issued based on a showing of probable cause.

- A governmental entity may access, or may require a covered entity to provide, prospectively or in real time, dialed number information, email to and from information or other data currently covered by the authority for pen registers and trap and trace devices only after judicial review and a court finding that the governmental entity has made a showing at least as strong as the showing under 18 U.S.C. 2703(d).

- Where the Stored Communications Act authorizes a subpoena to acquire information, a governmental entity may use such subpoenas only for information related to a specified account(s) or individual(s). All non-particularized requests must be subject to judicial approval.

DRAFT